



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/505,390	08/20/2004	Alain Durand	PF020015	7244

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/505,390	Applicant(s) DURAND, ALAIN	
	Examiner Devin Almeida	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4 and 5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4 and 5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 11/01/2007. Claims 1, 4 and 5 were received for consideration.

Response to arguments

Applicant's arguments filed 11/01/2007 have been fully considered but are not persuasive. With respect to claim 1 and 5, Ques et al teaches a secret specific to a second domain (i.e. the local private key Kpri.loc page 9 lines 28-34). The cable network sends data scrambled with cw these cw are transmitted in the data stream encrypted using key k (the key of the first network i.e. cable network). The access device 1 decrypts the encrypted cw using key k and re-encrypts the cw with the key is the second network the Kpub.loc of the Kpub.loc/Kpri.loc pair so only devices on the second network with the Kpri.loc can decrypt the data (page 8 lines 7-34). The second secret specific to said second domain (Kpub.loc) being different from said first secret specific to said first domain ((see page 7 line 31 - page 8 line 34 i.e. key k).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1, 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Quest et al (WO 00/62505) in view of Ford et al. (U.S. Patent # 5,481,613) rejected under 35

U.S.C. 102(b) as being anticipated by Quest et al (WO 00/62505). With respect to claim 1, a method of processing data, encrypted according to an encryption method specific to a first domain such that they data cannot be decrypted without the aid of a first secret specific to said first domain, said data being received in a presentation device connected to a network belonging to a second domain, wherein the method comprises the steps of:

(a) transmitting at least a portion of said encrypted data to a processing device (see figure 1 element 1 digital decoder and page 6 line 33- page 7 line 17 i.e. the digital decoder is connected either to a satellite antenna or a cable network, so as to receive video programs distributed by a service provider) connected to the network (see page 6 line 33- page 7 line 17 i.e. cable network) (see page 6 line 33- page 7 line 17 i.e. these program are received in a stream F of the for example in the MPEG-2 format. In a manner known per se, they are transmitted in scrambled form the content being scrambled by control words CW. These control words are themselves transmitted in the data stream F, in a form encrypted using key k according to the given enciphering algorithm in such a way as to remain secret during transmission); (b) receiving in said presentation device processed data (see page 8 lines 7-32 i.e. It is this data stream F' which will then flow around the domestic bus B so as to be received either by one of the presentation device 2 or 3 or by the digital video recorder 4 so as to be recorded) from said processing device (see figure 1 element 1 digital decoder sends F' to buss B), at least one element of said processed data being used by said presentation device to decrypt said received data using a second secret specific to said second domain (see page 8 lines 7-27 i.e. the converter 14 uses the key $K_{pub.loc}$ to encrypt the control words CW and transmits these control words, encrypted using the local public key to multiplexing circuit 15 in control messages denoted

LECM. These messages LECM have the same function as the message ECM received in the initial data stream F), said second secret being contained in the presentation device (see page 8 line 28-page 9 line 4 i.e. only apparatus containing the private local key $K_{pri.loc}$ of the network) said second secret (see page 9 line 28-34 i.e. the local private key $K_{pri.loc}$) specific to said second domain being different from said first secret specific to said first domain (see page 7 line 31 - page 8 line 34 i.e. key K); wherein the data received in the presentation device are encrypted with the aid of a first symmetric key (see page 6 line 32 - page 7 line 8 i.e. they are transmitted in scrambles form the content being-scrambled by control words CW), said first symmetric key (see page 6 line 32 - page 7 line 8 i.e. CW) being received with said data in a form encrypted with the aid of the first secret (see page 6 line 32 - page 7 line 8 these control words are them transmitted in the data stream F in a form encrypted using a key K); step (a) comprises transmitting to the processing device the first symmetric key encrypted with the aid of the first secret (see page 6 line 32 - page 7 line 8 these control words are them transmitted in the data stream F in a form encrypted using a key K); and step (b) comprises receiving from the processing device: said first symmetric key (see page 6 line 32 - page 7 line 8 i.e. CW) encrypted with the aid of a second asymmetric key (see page 8 line 7-27 i.e. the converter 14 uses the key $K_{pub.loc}$ to encrypt the control words CW and transmits these control words, encrypted using the local public key to multiplexing circuit 15 in control messages denoted LECM. These messages LECM have the same function as the message ECM received in the initial data stream F); (c) decrypting, with the aid of the second secret, the second encrypted asymmetric key (see Ford column 2 lines 45-67); (d) decrypting, with the aid of the second asymmetric key, the first encrypted symmetric key (see page 9 lines 13-34 i.e. the teminal

module can decrypt these control words using the local private key $K_{pri.loc}$ so as to obtain the control words CW in the clear); and (e) decrypting the data received by said presentation device with the aid of the first symmetric key (see page 9 lines 13-34 i.e. These control words CW are then transmitted to the descrambling circuit 24 which uses them to descramble the data packets DE and to output clear data packets DC to the television receiver 20); (e) decrypting the data received by said presentation device with the aid of the first symmetric key (see page 9 lines 13-34 i.e. These control words CW are then transmitted to the descrambling circuit 24 which uses them to descramble the data packets DE and to output clear data packets DC to the television receiver 20); and (f) transmitting a portion of data in the clear containing viewing control information indicative of a right of said presentation device to copy received data (see page 9 lines 13-34 i.e. These control words CW are then transmitted to the descrambling circuit 24 which uses them to descramble the data packets DE and to output clear data packets DC to the television receiver 20).

Ques does not teach the use of a second symmetric key and the second symmetric key encrypted with the aid of the second secret specific to the second domain. Ford teaches the use of a second symmetric key (see column 2 line 45-67 i.e. random symmetric key) and the second symmetric key encrypted with the aid of the second secret specific to the second domain (see column 2 line 45-67 i.e. Party A then generates a random symmetric key, and sends it to Party B, encrypted under Party B's public key). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the hybrid approach so that only Party B can learn the symmetric key value, as only Party B knows the private key needed to decipher the message (the encrypted symmetric key value).

Hence the two parties establish shared knowledge of the symmetric key, and can proceed to use it for protecting data communicated between them. Therefore one would be motivated to have replaced the asymmetric key of Ques with the hybrid approach discussed by Ford because of lower processing overheads and its particularly attractive for the bulk encryption/decryption of large volumes of data (see Ford column 2 lines 45-67).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ques et al. (WO 00/62505) in view of Ford et al. (U.S. Patent # 5,481,613) in further view of Rosen (U.S. Patent # 5,642,419). The above combination teaches everything with respect to claim 3 above, but with respect to claim 4, they do not teach generating a random number, the random number being transmitted to the processing device in step (a) with the encryption of the first symmetric key; and the data received in step (b) contains the random number and the first symmetric key encrypted with the aid of the second symmetric key; Step (d) also comprising the decryption, with the aid of the second symmetric, of the encrypted random number received in step (b); and the method also comprising, before step (e) verification step to verify that the random number decrypted in step (d) is identical to the random number generated before step (a); Step (e) being performed only in the event of positive verification. Rosen teaches generating a random number, the random number being transmitted to the processing device in step (a) with the encryption of the first symmetric key; and the data received in step (b) contains the random number and the first symmetric key encrypted with the aid of the second symmetric key; Step (d) also comprising the decryption, with the aid of the second symmetric, of the encrypted random number received in step (b); and the method also comprising, before step (e) verification step to

verify that the random number decrypted in step (d) is identical to the random number generated before step (a) (see Rosen column 35 lines 10-40). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have included a random number as to increase the security of the transactions. The random number ensures that old communications cannot be used in replay attacks therefore making a replay attack virtually impossible. Therefore one would have been motivated to include a random number to increase the security of the transactions by giving more confidence in the communication between domains (see Rosen column 35 lines 26-40).

With respect to claim 5, wherein a domain identifier is contained in the data received by the presentation device and in that said domain identifier is transmitted to the processing device during step (a) (see page 7 lines 9-17 i.e. the provider supplies the authorized users with the key K serving to decrypt the control words CW).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

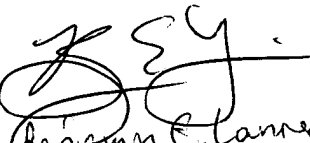
Application/Control Number:
10/505,390
Art Unit: 2132

Page 8

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
10/12/2007


Benjamin E. Lanner
Primary Examiner
AU 2132